**NSA**

**Install virtualization software**

Installed VirtualBox

Created new instance of a virtual machine:

A computer screen shot of a computer screen

AI-generated content may be incorrect.

A computer screen shot of a computer screen

AI-generated content may be incorrect.

A computer screen shot of a computer

AI-generated content may be incorrect.

A computer screen with a computer screen

AI-generated content may be incorrect.

I downloaded an Ubuntu image to use as the OS on my vm.

**Install and configure services**

For being able to use SSH and some of the other services, it is needed to go to the settings of the vm and change form NAT mode (default) to bridge node because if the vm is configured in NAT mode, it will receive its ip from the virtual box but with bridged mode it will receive directly from the main network (to which the host machine is also connected) so it will be easy to be accessed by other devices because it will act like a separate machine.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

* SSH

Install ssh: use first „sudo apt update” to be sure the system got the latest packages form Ubuntu, then for the installation use „sudo apt install openssh-server”

Enable the ssh server by: „sudo systemctl enable ssh”

Start it by: „sudo systemctl start ssh” and check again if it is running with „systemctl status ssh” (it should be using port 22)

Find the ip address of the VM: „ip a” and connect from the host machine to the VM using ssh

Run in command prompt „ssh username@ip” with username being ubuntu username (check Ubuntu username with „whoami”)

* WEB

„sudo apit upgrade”

„sudo apt install apache2” to install web server (to handle http requests)

„sudo systemctl enable apache2” to enable the server

„sudo systemctl start apache2” to start it

„systemctl status apache2” to check if it runs and „ss -tlnp | grep :80” if it is running on port 80

„<http://vm_ip>” in windows browser to check if it find the web server hosted by the vm

* FTP

„sudo apt update”

„sudo apt install vsftpd” to install ftp daemon server

„sudo systemctl enable vsftpd”

„sudo systemctl start vsftpd”

„systemctl status vsftpd” to check if it is running

„sudo nano /etc/vsftpd.conf” to open the config file with editor

Inside config file:

„anonymous\_enable=NO # disable anounymous login

local\_enable=YES

write\_enable=YES”

„chroot\_local\_user=YES # optional to restrict users to their home dir

allow\_writeable\_chroot=YES”

„pasv\_enable=YES # at the end of the file to enable passive mode for bridged networks

pasv\_min\_port=40000

pasv\_max\_port=50000”

„userlist\_enable=YES # limit access to some users

userlist\_file=/etc/vsftpd.userlist

userlist\_deny=NO”

„sudo systemctl restart vsftpd” restart the ftp for applying the new configuration

„sudo adduser ftpuser” create ftp user „sergiu\_goian” and set a password: „password”

„sudo mkdir -p /home/ftpuser/ftp” create a dedicated dir

„sudo chown ftpuser:ftpuser /home/ftpuser/ftp” change ownership of file,

„sudo chmod 750 /home/ftpuser/ftp” provide owner all perm and for the user group read + execute without write

„sudo ufw allow 21/tcp”

„sudo ufw allow 40000:50000/tcp”

„sudo ufw reload”

„sudo systemctl status vsftpd” check if it is running

„ftp localhost” and then give ftp username and password to check iff active, then „ls” to see if you can see ftp dir, then „bye” to exit

Test connection from host machine: type in file explorer in address bar „<ftp://vm_ip>”, then give user and pwd

Open command prompt: ftp <vm\_ip> and login

Or can also test using file zilla

Test from windows command: „ftp vm\_ip”

* DHCP

„sudo apt update’

„sudo apt install isc-dhcp-server” to install the dhcp server on vm

„sudo systemctl enable isc-dhcp-server” to enable it

„sudo systemctl start isc-dhcp-server” to start the service

„sudo nano /etc/dhcp/dhcpd.conf” to open config file

In the config file:

„default-lease-time 600;

max-lease-time 7200;

authoritative;

subnet 192.168.1.0 netmask 255.255.255.0 {

range 192.168.1.100 192.168.1.200;

option routers 192.168.1.1;

option domain-name-servers 8.8.8.8, 8.8.4.4;

}” adjust subnet and range based on network

„sudo nano /etc/default/isc-dhcp-server” edit default config to specify network interface for dhcp, find INTERFACESv4=”” and change to INTERFACESv4=”eth0” (use ip a to check interface name, most of the time ethernet0 but it could also be ens33)

Restart and check if it works: „sudo systemctl restart isc-dhcp-server”, „sudo systemctl status isc-dhcp-server”, and if errors check the logs by sudo journalctl -xe | grep dhcp

Check again in Newtork Settings if it is: virtBox settings -> newtork -> adapter1, needed to be bridged adapter (allowing the vm to act as a dhcp server in the real network)

Test from host: in cmd: „ipconfig /release” for realeasing existing ip, then renew ip using dhcp „ipconfig /renew”, then „ipconfig” and check if it is in the range specified in the config file; To reassign the old ip to the host, use again: „ipconfig /release” to remove the dhcp assigned ip, switch back to automatic (if network had another dhcp before) -> control panel -> networks an sharing center -> change adapter settings, right click on netwoek adapter -> select internet protocol V4 (TCP) -> properties -> obtain an ip addr automatically and OK, restart the network conneciton „ipconfig /renew”

* DNS

„sudo apt update „ , „sudo apt install bind9 bind9utils”

„sudo systemctl enable bind9”

„sudo systemctl start bind9”

„sudo systemctl status bind9”

„sudo nano /etc/bind/named.conf.options” to configure, add inside options{..} block this: „listen-on { any; };

allow-query { any; };”

„sudo nano /etc/bind/named.conf.local” and add „zone "example.com" {

type master;

file "/etc/bind/db.example.com";

};” to create domain example.com, create the dns records: „sudo cp /etc/bind/db.local /etc/bind/db.example.com”, „sudo nano /etc/bind/db.example.com” and add: „$TTL 86400

@ IN SOA example.com. root.example.com. (

2024032501 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

86400 ) ; Negative Cache TTL

@ IN NS ns1.example.com.

ns1 IN A 192.168.1.2 # Change to your VM's IP

www IN A 192.168.1.10 # Example web server”

„sudo systemctl restart bind9” to restart service

„sudo ufw allow 53/udp”, „sudo ufw allow 53/tcp”, „sudo ufw reload” to allow dns queries ni firewall

Test from host in cmd: „nslookup www.example.com <vm\_ip>”

* MAIL (port 25)

„sudo apt install postfix”

„sudo systemctl enable postfix”

„sudo systemctl start postfix”, select internet site, enter domain name ex.com

„sudo nano /etc/postfix/main.cf” to config postfix with: „myhostname = mail.example.com

mydomain = example.com

myorigin = /etc/mailname

inet\_interfaces = all

inet\_protocols = ipv4

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

mynetworks = 127.0.0.0/8, 192.168.1.0/24 # Adjust based on your network

home\_mailbox = Maildir/”

„sudo systemctl restart postfix” to restart the service and add a mail user: „sudo adduser mailuser” and set a pwd, create a maildir: „sudo mkdir -p /home/mailuser/Maildir”, „sudo chown -R mailuser:mailuser /home/mailuser/Maildir”,

„sudo chmod -R 700 /home/mailuser/Maildir”, allow smtp on port 25: „sudo ufw allow 25/tcp”, „sudo ufw reload”, send a mail: „echo "Test email from Postfix" | mail -s "Test Subject" [mailuser@example.com](mailto:mailuser@example.com)” and check it: „sudo -u mailuser mail”

Test from host: install telnet on host: „dism /online /Enable-Feature /FeatureName:TelnetClient”, open cmd and: „telnet <vm\_ip> 25”

* POP3/IMAP

„sudo apt install dovecot-core dovecot-imapd dovecot-pop3d”

„sudo systemctl enable dovecot”

„sudo systemctl start dovecot” and for config: „sudo nano /etc/dovecot/dovecot.conf” set „protocols = imap pop3”, config auth settings: „sudo nano /etc/dovecot/conf.d/10-auth.conf”: „disable\_plaintext\_auth = no

auth\_mechanisms = plain login”

Config mail directory: „sudo mkdir -p /home/ftpuser/Maildir”

„sudo chown -R ftpuser:ftpuser /home/ftpuser/Maildir”

„sudo chmod -R 700 /home/ftpuser/Maildir”

Restart: „sudo systemctl restart dovecot”, open firewall ports: „sudo ufw allow 110/tcp”,

„sudo ufw allow 995/tcp”, „sudo ufw allow 143/tcp”, „sudo ufw allow 993/tcp”, „sudo ufw reload”

Test pop3/imap in ubuntu: „telnet localhost 110”, „telnet localhost 143”, and from host: „telnet <vm\_ip> 110”, „telnet <vm\_ip> 143”

* Pop3S/IMAPS

„sudo apt install dovecot-core dovecot-imapd dovecot-pop3d -y”

„sudo systemctl enable dovecot”, „sudo systemctl start dovecot”, „sudo systemctl status dovecot”, edit the config: „sudo nano /etc/dovecot/dovecot.conf” and put: „protocols = imap pop3 lmtp” with: „disable\_plaintext\_auth = yes

auth\_mechanisms = plain login”, open firewall ports: „sudo ufw allow 995/tcp”, „sudo ufw allow 993/tcp”, „sudo ufw reload”, restart dovecot to apply config changes: „sudo systemctl restart dovecot”

test secured connection: „openssl s\_client -connect localhost:995”, „openssl s\_client -connect localhost:993”, and in host cmd: „openssl s\_client -connect <vm\_ip>:995”, „openssl s\_client -connect <vm\_ip>:993”

* Proxy

Install squid proxy: „sudo apt install squid -y”, „sudo systemctl enable squid”, „sudo systemctl start squid”, „sudo systemctl status squid”, config squid: „sudo nano /etc/squid/squid.conf” with:

„acl my\_network src 192.168.1.0/24

http\_access allow my\_network

http\_port 3128

access\_log /var/log/squid/access.log”, restart squid: „sudo systemctl restart squid”, open firewall ports: „sudo ufw allow 3128/tcp”, „sudo ufw reload”, test using curl: „curl -x http://<VM\_IP>:3128 -I http://www.google.com”

* Docker

„sudo apt install apt-transport-https ca-certificates curl software-properties-common -y”, add docker official gpg key: „curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo gpg --dearmor -o /usr/share/keyrings/docker-archive-keyring.gpg”, add docker repo: „echo "deb [arch=amd64 signed-by=/usr/share/keyrings/docker-archive-keyring.gpg] https://download.docker.com/linux/ubuntu $(lsb\_release -cs) stable" | sudo tee /etc/apt/sources.list.d/docker.list > /dev/null”, „sudo apt install docker-ce docker-ce-cli containerd.io -y”

„sudo systemctl enable docker”, „sudo systemctl start docker”, „sudo systemctl status docker”, verify docker installation: „sudo docker run hello-world”

* etc

**Administration tasks**

* monitor services availability (up or down)

„sudo apt install monit”, „sudo systemctl enable monit”, „sudo systemctl start monit”

„sudo nano /etc/monit/monitrc” and uncomment „set httpd port 2812 and

use address 0.0.0.0

allow 0.0.0.0/0”

„sudo systemctl restart monit”, then add services to monitor (ex ssh): „sudo nano /etc/monit/conf-enabled/ssh” and add this: „check process sshd with pidfile /run/sshd.pid

start program "/bin/systemctl start ssh"

stop program "/bin/systemctl stop ssh"

if failed port 22 protocol ssh then restart”, then „sudo systemctl restart monit”

* performance testing

„sudo apt install sysbench” for cpu testing, then „sysbench cpu –cpu-max-prime=20000 –threads=4 run”, for a longer test –cpu-max-prime needs increased

RAM test: „sysbench memory --memory-block-size=1M --memory-total-size=1G run”, increase to more Gb to testing more RAM

Disk: „sysbench fileio --file-total-size=5G prepare”

„sysbench fileio --file-total-size=5G --file-test-mode=randrw --threads=4 run”

„sysbench fileio cleanup”

Network: „sudo apt install iperf3”, run the server on vm: „iperf3 -s”, measure network speed between host and VM with: „iperf3 -c <vm\_ip>”

Stress: „sudo apt install stress”, and run test for cpu, ram, IO: „stress --cpu 4 --io 2 --vm 2 --vm-bytes 1G --timeout 60s”

* log analyzer

„sudo apt install logwatch”, to summarize logs and send daily reports

„sudo logwatch --detail high --mailto your-email@example.com --output mail”

OR

„sudo apt install goaccess” for live logs: „sudo goaccess /var/log/apache2/access.log --log-format=COMBINED” or „sudo goaccess /var/log/nginx/access.log --log-format=COMBINED”

* backup tasks

„sudo apt install rsync backuppc”

„rsync -av –delete /home /backup/” to sync home to backup, deleting old files in backup that no longer exist in home

**Security tasks**

* firewall

„sudo apt install ufw” to install uncomplicated firewall, „sudo ufw enable”, allow necessary ports: „sudo ufw allow 22/tcp” for ssh, „sudo ufw allow 21/tcp” for ftp, „sudo ufw allow 80/tcp

sudo ufw allow 443/tcp” for web server http + https, „sudo ufw allow 53/tcp

sudo ufw allow 53/udp” for dns, „sudo ufw allow 67/udp

sudo ufw allow 68/udp” for dhcp, deny everything else by default: „sudo ufw default deny incoming” and „sudo ufw default allow outgoing”

View firewall rules: „sudo ufw status verbose”, reload firewall: „sudo ufw reload”

If default settings needed (to not deny the other services): „sudo ufw reset”, „sudo ufw enable”, and then modify the default deny rule (without resetting everything): „sudo ufw default allow incoming”

* brute force detection/prevention

„sudo apt install fail2ban”, „sudo systemctl enable fail2ban”, „sudo systemctl start fail2ban”

Config fail2ban, so create a local override file to prevent updates form overwriting changes: „sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local”, edit the config file: „sudo nano /etc/fail2ban/jail.local”

Add this:

„bantime = 10m

findtime = 10m

maxretry = 5

ignoreip = 127.0.0.1”, and for ssh brute force protection: „[sshd]

enabled = true

port = 22

filter = sshd

logpath = /var/log/auth.log

maxretry = 3

bantime = 15m”

„sudo systemctl restart fail2ban”, then check active jails: „sudo fail2ban-client status”, check sttus of ssh jail: „sudo fail2ban-client status sshd”, check if an ip is banned: „sudo fail2ban-client banned”

Test fail2ban connecting via ssh from host machine („ssh <ubuntu-username>@<ubuntu-vm-ip>”) and enter wrong password, so after 3 failed attempts as configured, your ip should be banned, verify if banned: „sudo fail2ban-client status sshd” and to unban an ip: „sudo fail2ban-client set sshd unbanip <ip>”